REMARKS / ARGUMENTS

The present application includes pending claims 1-41, all of which have been rejected. The Applicant respectfully submits that the claims define patentable subject matter.

Independent claims 1, 11, 21, and 32 have been amended. Support for the claim amendments may be found in, for example, FIG. 6A and paragraphs 46-54 of the specification.

Claims 1-41 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0001386, issued to Akiyama (hereinafter, Akiyama), in view of U.S. Patent No. 6,073,237, issued to Ellison (hereinafter, Ellison).

The Applicant respectfully traverses these rejections at least for the reasons previously set forth during prosecution and at least based on the following remarks.

I. Examiner's Response to Arguments

The Examiner states the following in page 3 of the Office Action:

> Examiner would like to further point out that applicant is trying to force examiner to read the claim such that it would require a secure key and a key that encrypts secure key to be of same type. However, examiner is interpreting the current language of the claim such that as long as the key that encrypt the secure key is also a secure key it reads onto the claimed limitation. Since the master key of Akiyama is only provided to the subscriber through smart cards, the master key of Akiyama is in fact a "secure key". Therefore, the combination of Akiyama and Ellison still

> discloses all the limitations and the rejection is maintained. Note: examiner would like to further point out that the interpretation taken by applicant that claim require work key to be encrypted using previously generated work keys are not even supported by the specification. Throughout the specification, particularly page 5, lines 22-25 recites, " For example, in the CA system 100 illustrated in FIG. 1, the content scrambling key 118 is protected by the work key 122, which is in turn protected by the master key 126. This key protection "chain" is, sometimes, referred to as a key ladder". Further note that the invention is of a key ladder wherein lower level keys are encrypted using higher level keys. Nowhere in the specification it is recited that same level keys are encrypted using the same level keys as argued by the applicant.

The Applicant submits that claim 1, as presented in the 08/11/08 response, indeed required that a secure key and a key that encrypts the secure key to be of same type. However, to further prosecution and to further clarify this aspect, the Applicant has amended independent claims 1, 11, 21 and 32, as set forth above. Support for the claim amendments may be found, for example, in Fig. 6A and paragraphs 46-54 of the specification.

More specifically, referring to Applicant's Fig. 6A, the digitally signed secure keys 638 are encrypted by the encryptor 608. The encrypted and signed secure keys 632 are looped back via the registers 610 and then communicated back (628 and 630) to the encryptor 608 for purposes of encrypting the next digitally signed secure key. Obviously, the digitally signed secure keys and the encrypted digitally signed secure keys are of the same type, the difference being that the latter have been encrypted and then looped back for purposes of using them during encryption of subsequent signed secure keys.

In the above citation, the Examiner refers for support to Fig. 1 and page 5, lines 22-25 of the specification. The Examiner further states: "the invention is of a key ladder wherein lower level keys are encrypted using higher level keys. Nowhere in the specification it is recited that same level keys are encrypted using the same level keys as argued by the applicant." The Applicant respectfully disagrees with such characterization of Applicant's invention. The Examiner is encouraged to carefully read the entire specification in light of all Figures. The Applicant is puzzled as to why the Examiner even uses Fig. 1 and page 5 of the specification to judge what Applicant's invention is, since FIGS. 1-4 were clearly marked as PRIOR ART, and pages 1-10 constitute the "Background of the Invention" section. The detailed description of the invention is in pages 15-24 and FIGS. 5-6B of the specification (the Applicant has already briefly summarized Fig. 6A and why the secure key and the key that encrypts the secure key are of the same type).

REJECTION UNDER 35 U.S.C. § 103

In order for a *prima facie* case of obviousness to be established, the Manual of Patent Examining Procedure, Rev. 6, Sep. 2007 ("MPEP") states the following:

> The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR International Co. v. Teleflex Inc., 82 USPQ2d 1385, 1396 (2007) noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere

> conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."

See the MPEP at § 2142, citing *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006), and *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d at 1396 (quoting Federal Circuit statement with approval). Further, MPEP § 2143.01 states that "the mere fact that references can be combined or modified does not render the resultant combination obvious unless the results would have been predictable to one of ordinary skill in the art" (citing *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007)). Additionally, if a *prima facie* case of obviousness is not established, the Applicant is under no obligation to submit evidence of nonobviousness.

> The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

See MPEP at § 2142.

II. The Proposed Combination of Akiyama and Ellison Does Not Render Claims 1-41 Unpatentable

The Applicant now turns to the rejection of claims 1-41 as being unpatentable over Akiyama in view of Ellison. The Applicant notes that the proposed combination of Akiyama and Ellison forms the basis for all of the pending rejections.

A. Independent Claims 1, 11, 21, and 32

With regard to the rejection of independent claim 1 under 103(a), the Applicant submits that the combination of Akiyama and Ellison does not disclose or suggest at least the limitation of "encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key," as recited by the Applicant in independent claim 1. The Office Action states the following:

> Regarding Claim 1, Akiyama discloses a method for secure key authentication, the method comprising:
>
> generating at a first location (Fig.29, This is a broadcast station where the contents, keys and digital signature for contact information etc, are generated and then sent to receivers) a digital signature (Fig. 5, "Digital signature") of a secure key to obtain a digitally signed secure key (Fig. 5, "work keys", also at paragraph 0107, "The digital signature is information used to check the " authenticity of the contract information, and is used to prevent tampering.", also at paragraph 0107, "The contract information is made up of, e.g., a receiver 10, channel contract information, the number n of work keys, n pairs of work keys and work key identifiers, and digital signature").
>
> encrypting the digitally signed secure key utilizing at least a previously generated unreadable key (Fig. 7, "Enciphered contract information", also at Paragraph 0106, lines 5-8, "The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7.", Note: *[Each digitally signed contract information is encrypted using a master key, also note that master keys are generated and sent to clients via secure card therefore master keys are generated prior to encrypting work keys and it is also unreadable and also secure because only broadcaster and receivers have the master key (see Paragraph 0154))*

See the Office Action at pages 4-5. The Examiner has used Ellison to teach that a key can be encrypted and signed. Even if we assume that Ellison is combinable with Akiyama (and assume Akiyama's keys can be encrypted and signed), the Applicant points out that Akiyama is still deficient at least for the following reasons.

Referring to FIG. 5 of Akiyama, the Examiner has equated Applicant's "secure key" to Akiyama's "work key", which is part of Akiyama's contract information. Furthermore, Akiyama discloses that a separate master key is used to encrypt the work key, as illustrated in FIG. 3 and further explained in paragraph 0100 of Akiyama. **However, the work keys of Akiyama are different from the master keys, which are used for encrypting the work keys. More specifically, Akiyama's master key is not a previously encrypted and signed work key (i.e., the master key is not generated by encrypting a previously generated signed work key).**

In this regard, Akiyama does not disclose that the work keys (equated by the Examiner to Applicant's "secure key") are encrypted utilizing a previously generated unreadable digitally signed and encrypted work key, where the previously generated unreadable digitally signed and encrypted work key was generated by encrypting a previously generated signed work key. In other words, Akiyama does not disclose that the work keys are encrypted using previously generated work keys, as recited in Applicant's claim 1. Ellison does not overcome the above deficiencies of Akiyama.

Therefore, the Applicant maintains that the combination of Akiyama and Ellison does not disclose or suggest at least the limitation of "encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key," as recited by the Applicant in independent claim 1.

Accordingly, the proposed combination of Akiyama and Ellison does not render independent claim 1 unpatentable, and a *prima facie* case of obviousness has not been established. The Applicant submits that claim 1 is allowable. Independent claims 11, 21, and 32 are similar in many respects to the method disclosed in independent claim 1. Therefore, the Applicant submits that independent claims 11, 21, and 32 are also allowable over the references cited in the Office Action at least for the reasons stated above with regard to claim 1.

B. Rejection of Dependent Claims 2-10, 12-20, 22-31, and 33-41

Based on at least the foregoing, the Applicant believes the rejection of independent claims 1, 11, 21, and 32 under 35 U.S.C. § 103(a) as being unpatentable over Akiyama in view of Ellison has been overcome and requests that the rejection be withdrawn. Additionally, claims 2-10, 12-20, 22-31, and 33-41 depend from independent claims 1, 11, 21, and 32, respectively, and are, consequently, also respectfully submitted to be allowable.

The Applicant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 2-10, 12-20, 22-31, and 33-41.

In general, the Office Action makes various statements regarding claims 1-41 and the cited reference that are now moot in light of the above. Thus, the Applicant will not address such statements at the present time. However, the Applicant expressly reserves the right to challenge such statements in the future should the need arise (e.g., if such statement should become relevant by appearing in a rejection of any current or future claim).

CONCLUSION

Based on at least the foregoing, the Applicant believes that all claims 1-41 are in condition for allowance. If the Examiner disagrees, the Applicant respectfully requests a telephone interview, and requests that the Examiner telephone the undersigned Attorney at (312) 775-8176.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

A Notice of Allowability is courteously solicited.

Respectfully submitted,

Date: March 2, 2009

/Ognyan I. Beremski/

Ognyan Beremski, Esq.
Registration No. 51,458
Attorney for Applicant

McAndrews, Held & Malloy, Ltd.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
(312) 775-8000

/ OIB